

UNITED STATES DISTRICT COURT

for the
District of New Mexico

FILED

United States District Court
Albuquerque, New MexicoMitchell R. Elfers
Clerk of Court

In the Matter of the Search of _____
*(Briefly describe the property to be searched
or identify the person by name and address)* }
 TWITTER ACCOUNTS @VotePatrickBeck; }
 @Patrick55894453; @Sluttybitches3; THAT IS STORED }
 BY TWITTER INC }

Case No. 22-MR-992

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See attachment A, attached hereto and incorporated herein.

located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC 2261A

Stalking

Offense Description

The application is based on these facts:

See Affidavit, attached hereto and incorporated herein

Continued on the attached sheet.

Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Eric Bruce, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone _____ (*specify reliable electronic means*).

Date: June 24, 2022

City and state: Albuquerque, New Mexico

Karen B. Molzen, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH:
TWITTER ACCOUNTS @VotePatrickBeck;
@Patrick55894453; @Sluttybitches3; THAT
IS STORED AT PREMISES CONTROLLED
BY TWITTER, INC.

Case No. 22-MR-992

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Eric Bruce, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Twitter, Inc. (Twitter), an online communications provider headquartered at 1355 Market Street, Suite 900, San Francisco, CA.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Twitter to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since January, 2019. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime. I have gained experience through training

and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I earned Bachelor's degrees in Mathematics and Economics and a Master's degree in International Affairs. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2261A, and I am authorized by the Attorney General to request a search warrant.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2261A (Stalking) exists in the Twitter accounts @VotePatrickBeck; @Patrick55894453; and @Sluttybitches3 (collectively, the SUBJECT ACCOUNTS). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background & Terms

1. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

2. 18 U.S.C. § 2261A criminalizes conduct by which someone “with the intent to kill, injure, harass, intimidate...uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that...places that person in reasonable fear of the death of or serious bodily injury or...causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress.” A “course of conduct” is described as “two or more acts, evidencing a continuity of purpose”.

Summary of Investigation to Date

1. On or about May 7, 2022, I identified a complaint filed by DW, a resident of Texas, with the Internet Crime Complaint Center (IC3). The IC3 is a government organization that supplies the public with a reporting mechanism to provide information to the FBI regarding suspected internet-facilitated criminal activity. In the complaint, DW alleged she was being stalked, harassed, and threatened by Patrick Beck, a resident of Albuquerque, New Mexico. DW

alleged Beck used online social media to send her threatening and harassing messages as well as make public posts about her.

2. I communicated with DW via email regarding the complaint. DW further explained that BECK had been “catfished” online by someone using her publicly available photos. I understand the term “catfish” to refer to the use of photos belonging to another person to trick someone into an online relationship. DW was a model on Instagram and made pictures of herself publicly available. According to DW, BECK identified her real accounts, became obsessed with her, and believed they had been married. DW did not know BECK and did not have a relationship with him. When DW told BECK to stop contacting her, BECK started sending harassing and threatening messages. This conduct continued for approximately a year. DW also explained that her friend, DW2¹, a resident of Michigan, had become the target of abuse as well.

3. Following my communication with DW, I identified a complaint, filed by DW2 on or about February 8, 2022, with the FBI’s National Threat Operations Center (NTOC). in the complaint, DW2 alleged that BECK targeted him because he was associated with DW on social media. DW2 alleged BECK had threatened DW2 and DW2’s family with injury, death, and rape starting in February 2022. DW2 further alleged BECK had posted personal details about DW2 using multiple social media accounts including DW2’s address, phone number, family members, and photos along with messages imploring others to injure and/or harass DW2 and DW2’s family.

¹ DW2 is a person, known to the FBI, who bears the same initials as complainant DW but bears no familial relationship to DW.

4. On or about May 18, 2022, DW2 contacted me by phone and informed me that DW had died, apparently of suicide, some days prior. DW2 opined BECK's ongoing harassment of DW may have contributed to her suicide.

5. I obtained and reviewed a driver's license photograph of BECK on or about May 25, 2022 from the FBI Albuquerque operations center.

6. Between approximately May 7, 2022 and June 3, 2022, DW2 communicated with me via email and provided me with numerous screenshots of messages and social media posts allegedly made by BECK using several Twitter accounts, several of which appeared to have been created for the purpose of sending messages to DW2. In many of the messages, the user of the account(s) alleges that DW2 initiated the harassment, a fact which DW2 denied in email communications to me.

7. On or about June 2, 2022, I reviewed the screenshots provided by DW2 and identified the SUBJECT ACCOUNTS. In the following sections, DW and DW2's names are redacted from representations of the Twitter posts and messages. DW's name and related information is redacted in blue and DW2's name and related information is redacted in red.

DETAILS OF TWITTER ACCOUNT @VotePatrickBeck

8. On or about June 2, 2022, I reviewed screenshots of communications provided by DW and DW2 purportedly showing messages or public posts sent from the Twitter account @VotePatrickBeck to DW2 and identified the following representative messages and posts:

10:18

Patrick Beck 449 Tweets

Tweets Tweets & replies Media Likes

@askredditTravel and 2 others

[REDACTED] has pissed me off for the last time and she threatened me. So in my defense. We shall attack and conquer until they are all dead or in jail.

Replying to @philo866866
@askredditTravel and 2 others

I know their information and weaknesses. We can attack them in ways that you could never imagine. She doesn't want to surrender so we must fight back and attack them as ruthlessly as they have done to me until there are none of them left. I was nice before now.

Replying to @philo866866
@askredditTravel and 2 others

She is but then [REDACTED] got his sick twisted mind into her and then she flipped on me because of him. They keep reporting my accounts. If you want to get [REDACTED], you'll have to take [REDACTED] out right away. Harass him nonstop and expose him for the sorry SOB he is.

a.



Patrick Beck @VotePatrickB... · 4/9/22 ...

Replies to [@philo866866](#)

[@askredditTravel](#) and 2 others

I don't trust you. You are trying to ruin my relationship with [REDACTED] and it's clear as day. But if you are working for me, that's another thing. I'll give you all of [REDACTED]'s information. It's only fair after what he did to me. You want to know where his kids go to school at?



b.



Patrick Beck @VotePatrickBeck · 16h ...

Replies to [@philo866866](#) and [REDACTED]

Well [REDACTED] Lives in Michigan for starters. He has two kids and a wife named Kasey. He likes to stalk and troll people so he can clown on them online.



c.

i. According to DW2, this message was posted April 10, 2022.



Patrick Beck

@VotePatrickBeck

Replies to [@philo866866](#) @ralkthar and 4 others

This is [REDACTED] and his number. Leave me alone. He has kids and a wife. See he says so right there.



531



d.

i. According to DW2, this message was posted April 12, 2022. DW2's personal phone number was posted and redacted at the bottom of this message.



Patrick Beck @VotePatrickBeck · 1m

[REDACTED] will burn in hell for the torture he has caused these poor and innocent souls.



e.

i. According to DW2, this message was posted April 18, 2022.



Patrick Beck @VotePatrickBeck · 21m

I heard that [REDACTED] is a rapist who molested his children and beat up his wife [REDACTED] who is also facing convictions for medical malpractice and needs to be put under investigation.

@MichiganDems @UMich #rapist

#medicalmalpractice #michigan

@CDCDirector



f.

i. According to DW2, this message was posted May 5, 2022.

DETAILS OF TWITTER ACCOUNT @Patrick55894453

9. On or about June 2, 2022, I reviewed screenshots of communications provided by DW and DW2 purportedly showing messages or public posts sent from the Twitter account @Patrick55894453 to DW2 and identified the following representative messages and posts:



Patrick Beck
@Patrick55894453

Replying to @Patrick55894453 @pappyslappyhand
and 5 others

[REDACTED] is a delusional
methed out racist pedophile with
schizophrenia who likes to stalk
celebrities and threaten them. He was
2 kids and a wife. Maybe we should
doxx him just for the hell of it. I have
his address and phone number.
Where that guy who wanted to rape
her?

a. 9:18 AM · 3/26/22 · Twitter for iPhone



Patrick Beck
@Patrick55894453

Replying to [REDACTED]

[REDACTED] how are your kids
and your wife Casey. You nasty child
molester. You deserve to have your
kids taken away and put into foster
care while you spend the rest of your
life behind bars for rape and child
torture/molestation. You still live in
Massachusetts? @FBI

b. 9:30 AM · 3/26/22 · Twitter for iPhone

DETAILS OF TWITTER ACCOUNT @Sluttybitches3

10. On or about June 2, 2022, I reviewed screenshots of communications provided by DW2 purportedly showing messages or public posts sent from the Twitter account @Sluttybitches3 to DW2 and identified the following representative messages and posts:



Slutty bitches @Sluttybitches3 · 17m

[REDACTED] IS A PATHETIC
LOSER AND DESERVES TO GET SHOT IN
THE HEAD. HE IS A RAPIST AND A METH
FIEND.

...

c.



- i. According to DW2, this message was posted on Twitter on or about April 11, 2022, approximately two days after the initial contact from BECK.
- ii. Based on the similarity of the verbiage of this message to those posted by account @Patrick55894453 and the proximity in time, it is reasonable to believe that it was posted by the same individual using the accounts described elsewhere in this affidavit.

11. Based on the content of this message and the likelihood that this account was created or operated by the same individual as the accounts listed above, I have probable cause to believe that evidence of violations of 18 U.S.C. 2261A exists in the account @Sluttybitches3.

SUMMARY

12. Based on my training and experience, I know that online communication providers, like Twitter, collect information regarding the users of such communication accounts that may tend to identify the user of the account. I also know that a comprehensive review of the contents of such accounts may provide valuable context regarding the sending and receiving of harassing communications that may either inculpate or exculpate the sender or the messages.

BACKGROUND CONCERNING TWITTER²

1. Twitter owns and operates a social networking and microblogging service of the same name that can be accessed at <http://www.twitter.com> and via the Twitter mobile application (“app”). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.

2. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called “Tweets,” with the public or, alternatively, to “protect” their Tweets by making them viewable by only a preapproved list of “followers.” Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets (“retweet”) or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.

3. Twitter also permits its users to exchange private messages, known as “direct messages” or “DMs,” with other Twitter users. DMs, which also may include photos, videos, links, and/or text, can only be viewed by the sender and designated recipient(s). Direct messages may be sent to an individual user or to a group of up to 50 Twitter users. Twitter users have the ability to choose whether they can receive a direct message from anyone. At any time, a Twitter user has the ability to alter the settings on their Twitter account so that they can receive direct

² The information in this section is based on my training and experience, and on information published by Twitter on its website, including, but not limited to, the following webpages: “Data Policy,” available at <https://help.Twitter.com/519522125107875>; “Information for Law Enforcement,” available at <https://help.Twitter.com/494561080557017>; and “Help Center,” available at <https://help.Twitter.com>.

messages only from (1) individuals to whom the user has already sent a direct message and (2) Twitter accounts that the user “follows” via his account.

4. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to “follow” accounts in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter’s website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique user ID (“UID”). A user must also select a password as well as a unique Twitter username (also known as a “handle”). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username (for example: @example). The user may also select a different name (the “display name”), which is not automatically preceded by the @ symbol, to be displayed on his profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change their password, username, and/or display name at any time, but the UID for the account will remain constant.

5. While anyone can sign up and use Twitter for free, as of November 2021 Twitter also offered a subscription model that offered users access to additional features and app customizations. This new subscription is called Twitter Blue. A user can sign up for Twitter Blue at any time.

6. At the time of account creation, Twitter asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. Twitter also keeps certain information relating to the creation of each Twitter account, including: (1) the date and time at which the user’s account was created; and (2) the method of account creation (e.g., website or Twitter app).

7. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information including (1) the user's Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved "followers"). The user can personalize this page by posting a personal picture or image (known as an "avatar") to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify his location, to provide a link to his website, or to specify his date of birth.

8. As noted above, Twitter users can use their account to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as a "mention." The Twitter user mentioned in the Tweet will receive a notification informing them that they have been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will receive a notification that someone replied to their message, and the notification will show the content of that reply.

9. Twitter users can also include links to webpages in their Tweets and Direct Messages. Twitter automatically processes and shortens links provided by the user to a shortened link that starts <http://t.co/>. Twitter tracks how many times these shortened links are clicked.

10. A registered Twitter user can also "like" a Tweet by clicking a heart icon on a Tweet sent by another user. If another user "likes" a Tweet that is posted by the Twitter user, a notification will appear in the user's account identifying what Tweet was liked and who liked it.

11. As noted above, users can include photographs, images, and videos in their Tweets. Each account has a “media timeline” on their profile that displays “the photos, videos, and GIF’s [the accountholder] has uploaded with [their] Tweets.” An individual can view a Twitter user’s media timeline by visiting the user’s Twitter profile page.

12. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt-in to utilize it. However, if a Twitter user enables Twitter to access their precise location information, the Twitter user will have the option of attaching their location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter’s in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user’s choice as well as the device’s precise location in the form of latitude-longitude coordinates. The user can turn this functionality off (thereby removing their location from their Tweets) at any time, and they can delete their past location data from Tweets that have already been sent.

13. A Twitter user may choose to “follow” another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the “follow” button on the other user’s Twitter profile page. If a Twitter account is protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the “follow” button and waiting for the other user to approve their request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the user’s Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform them about the new follower. Each user’s Twitter profile page includes a list of the people who are following that

user and a list of people whom that user follows. Twitter users can “unfollow” other users whom they previously followed at any time. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

14. A Twitter user can also “block” other Twitter users. This prevents the blocked account from contacting or following the user or from seeing the user’s Tweets. Twitter does not notify the user of a blocked account when another Twitter account blocks them.

15. A Twitter user can also use Twitter’s integrated search function. When a user types a search term into Twitter’s search tool, it will return results that include accounts, Tweets, and photos that match that search term. Twitter users using the service via the Twitter mobile app also have the option of saving searches that they have performed. A user can delete such saved searches at any time.

16. A Twitter user can also join or create “Lists” of other Twitter accounts. These Lists often organize Twitter accounts by group, topic, or interest. Viewing a timeline of a specific List will show you a stream of Tweets made only by accounts that are on that List. Users can pin their favorite lists to their Twitter Home timeline page. Twitter users have the ability to remove their accounts from Lists upon which it may appear.

17. Twitter also offers a functionality called “Spaces,” which it calls “a new way to have audio conversations on Twitter.” Any user can create a Space; that user is referred to as the “host.” Spaces are public, so anyone can join and listen to the conversation within a Space once it is created, although a user can send another Twitter user a link to their Space and invite them to join. By default, the only individuals permitted to speak in a Space are the individuals that the

host invites to do so, although this setting can be modified to allow a broader set of individuals to speak. Up to 13 people can be in a Space at a given time.

18. Twitter also offers the ability to sign into third-party apps and websites using one's Twitter account. Typically, the third-party app or website will have a link that enables the user to sign into the third-party service using their Twitter account. Doing so grants the third-party service access to the Twitter user's account. Depending on the authorizations the Twitter user gives to the third-party service, the third-party service may be able to read the user's Tweets, see who the user follows on Twitter, post Tweets to the user's profile, or access the user's email address. A user can revoke a third-party app or website's authorization to access their Twitter account and associated data at any time.

19. Twitter collects and retains information about a user's use of the Twitter service, to include: (1) content of and Twitterdata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user's Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user's account; (4) the content uploaded to a user's profile page, including their avatar, banner image, and bio; (5) information about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected to the Twitter account. Twitter also collects and retains various other data about a user and his/her activity, including:

- a. logs of Internet Protocol ("IP") addresses used to login to Twitter and the timestamp associated with such logins;

- b. transactional records reflecting, for example, when a user changed their display name or email address;
- c. the identities of accounts that are blocked or muted by the user; and
- d. information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.

20. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

21. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other things, the browser being used, its version number, and details about the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user's browser and operating system.

22. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion

23. Based on my training and experience, public posts, direct messages, and photos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

24. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Twitter can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos, and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

26. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

27. Therefore, Twitter's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

13. Based on the aforementioned information and investigation, it is reasonable to believe that the SUBJECT ACCOUNTS will contain records and evidence of violations of 18 U.S.C. § 2261A including harassing or threatening messages, the identity of the user of the accounts, and additional context regarding the messages. Moreover, it is reasonable to search the contents of The SUBJECT ACCOUNTS for evidence of stalking as well as for information corroborating the identity of the user(s) of the SUBJECT ACCOUNTS and their state of mind regarding intent. Because some of this information may have been stored in the accounts at any point in time, it is reasonable to review the entire contents of the SUBJECT ACCOUNTS.

14. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Twitter who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

15. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Eric Bruce
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me via telephone or other reliable electronic means on
June 24, 2022



Karen B. Molzen _____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

This warrant applies to information associated with Twitter account @VotePatrickBeck; @Patrick55894453; and @Sluttybitches3 (collectively, the SUBJECT ACCOUNTS), that is stored at premises owned, maintained, controlled, or operated by Twitter, Inc. a company headquartered at 1355 Market Street, Suite 900, San Francisco, CA.

KBM

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Twitter, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, Inc., regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Twitter, Inc., Twitter, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A from account creation to present:

- A. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNTS, including:
 1. Identity and contact information (past and current), including full name, email addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 2. All Twitter usernames (past and current) and the date and time each username was active, all associated Twitter accounts (including those linked by machine cookie), and all records or other information about connections with Twitter, third-party websites, and mobile apps (whether active, expired, or removed);
 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

KBM

4. Devices used to login to or access the SUBJECT ACCOUNTS, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
6. Internet Protocol (“IP”) addresses used to create, login, and use the SUBJECT ACCOUNTS, including associated dates, times, and port numbers;
7. Privacy and account settings, including change history; and
8. Communications between Twitter and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the SUBJECT ACCOUNTS), records, and other information relating to videos (including live videos), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and Twitter data;

C. All content, records, and other information relating to communications sent from or received by the SUBJECT ACCOUNTS including but not limited to:

1. The content of all communications sent from or received by the SUBJECT ACCOUNTS, including direct and group messages, and all associated multimedia and Twitter data, including deleted and draft content if available;

KBm

2. All records and other information about direct, group, and disappearing messages sent from or received by the SUBJECT ACCOUNTS, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
4. All associated logs and Twitter data;

D. All content, records, and other information relating to all other interactions between the SUBJECT ACCOUNTS and other Twitter users, including but not limited to:

1. Interactions by other Twitter users with the SUBJECT ACCOUNTS or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
2. All users the SUBJECT ACCOUNTS has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
3. All contacts and related sync information; and
4. All associated logs and Twitter data;

1CBM

- E. All records of searches performed by the SUBJECT ACCOUNTS; and
- F. All location information, including location history, login activity, information geotags, and related Twitter data.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2261A, those violations involving Patrick BECK, DW, DW2, or other persons yet unidentified, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Threats to harm or injure;
- (b) Communications that would cause, attempt to cause, or be reasonably expected to cause substantial emotional distress;
- (c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- (d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- (e) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

KBm

staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

KBM

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS

PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Twitter, and my official title is _____. I am a custodian of records for Twitter. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Twitter, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Twitter.; and
- c. such records were made by Twitter as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

